ROYAUME DE BELGIQUE



COMMISSION DE LA PROTECTION DE LA VIE PRIVEE

Adresse : Rue Haute, 139, B-1000 Bruxelles
Tél. : +32(0)2/213.85.40
Fax : +32(0)2/213.85.65
E-mail : commission@privacycommission.be
Site Internet : http://www.privacycommission.be

AVIS N° 37 / 2006 du 27 septembre 2006

N. Réf. : SA2 / A / 2006 / 035

OBJET : Avis relatif à la transmission de données à caractère personnel par la SCRL SWIFT suite aux sommations de l'UST (OFAC)

La Commission de la protection de la vie privée ;

Vu la Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* (ci-après la "Directive 95/46/CE") ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après la "LVP"), en particulier l'article 29, § 1 ;

Vu la demande d'avis du Collège du renseignement et de la sécurité du 6 juillet 2006, reçue par la Commission le 19 juillet 2006 ;

Vu la correspondance avec SWIFT ;

Vu le rapport de Monsieur De Schutter ;

Emet, le 27 septembre 2006, l'avis suivant :

A. INTRODUCTION

Le 19 juillet 2006, la Commission a reçu du Collège du renseignement et de la sécurité une demande d'avis sur "la question de savoir si, dans le cadre du dossier "SWIFT", il était question d'une violation de la législation belge, plus spécifiquement de la LVP". Il a également été demandé à la Commission de mettre à la disposition du Collège tous les éléments pouvant être utiles pour remplir son mandat.

Lors de sa séance du 5 juillet 2006, la Commission avait déjà décidé d'ouvrir d'office une enquête dans ce dossier, sur la base de l'article 32, § 1 de la LVP[1], concernant le traitement de données à caractère personnel sous la responsabilité de SWIFT, sur la base de divers communiqués de presse parus fin juin[2] quant au rôle de SWIFT lors de la transmission de données à caractère personnel à l' "US Department of the Treasury" (UST), plus précisément l' "Office of Foreign Assets Control" (OFAC). SWIFT est une société coopérative de droit belge, dont le siège social est établi en Belgique, ayant une responsabilité limitée (SCRL)

La Commission a enfin pris connaissance, le 28 juin 2006, d'une plainte publique formulée par l'organisation "privacy International" à l'égard des autorités et régulateurs de protection des données de 33 pays concernant les communiqués de presse évoqués ci-avant.

L'enquête de la Commission s'est exclusivement concentrée sur la problématique susmentionnée et ne concernait donc pas les traitements de données à caractère personnel propres aux activités administratives ou de management normales d'une entreprise (administration du personnel, gestion de la clientèle, etc.). La Commission constate ici que SWIFT a effectué quant à ces derniers traitements les déclarations nécessaires auprès de la CPVP, selon les prescriptions de la LVP. L'attention a dès lors été attirée sur le flux de données via le service "SWIFTNet FIN" et sur la communication à l'UST de données qui sont générées via ce service. Concernant d'autres services, la Commission n'a pas connaissance d'un transfert de données à l'UST.

Pour rédiger le présent avis, la Commission s'est basée sur les informations publiques de SWIFT[3], sur de la documentation pour laquelle SWIFT a accordé un droit de consultation à la Commission (application de l'article 31, § 1 de la LVP), sur des éléments issus de demandes de renseignements répétées[4] et d'informations obtenues lors de réunions de concertation avec des responsables de SWIFT (conseiller général ou "general counsel", président-directeur ou "CEO", responsable audit, service juridique, conseillers juridiques) le 23 août et le 31 août (examen sur place) et enfin sur des éléments des réunions internes de la Commission des 6 et 27 septembre 2006.
Parallèlement, une demande de renseignements écrite a également été adressée à la Banque nationale de Belgique par lettre du 10 août 2006.

---

[1] Dans un avis du 13 novembre 1996 relatif à l'avant-projet de loi adaptant la loi du 8 décembre 1992 à la Directive 95/46/CE, on peut lire que la Commission se considère compétente pour effectuer des contrôles sur place d'initiative ou sur plainte ou sur la base de la déclaration de traitements très sensibles.

[2] Principalement le New York Times ("bank Data is sifted by US in secret to block terror" du 22 juin 2006), (www.nytimes.com), le International Herald tribune ("oversight on records defended" du 25 juin 2006), le Los Angeles Times ("secret US Program tracks global bank transfers" du 23 juin 2006) et, y faisant suite, des réactions de la presse dans le monde entier.

[3] Principalement les informations sur le site Internet de SWIFT www.swift.com et d'autres informations imprimées.

[4] Lettre de la CPVP du 7 juillet et réponse de Swift du 28 juillet.
Lettre de la CPVP du 8 septembre et réponse de Swift du 14 septembre 2006.

Mentionnons enfin que la problématique de la transmission à l'UST est également traitée actuellement au sein de l'Union européenne[5] et auprès de certaines autorités de protection des données ("DPA") au sein et en dehors de l'Europe (Allemagne, Italie, France, Canada, Australie, etc.).

La Commission s'est concertée à ce sujet avec le groupe européen de protection des personnes à l'égard du traitement des données à caractère personnel, créé sur la base de l'article 29 de la Directive 95/46/CE (dénommé ci-après le “Groupe 29”). Le Groupe 29 a d'ores et déjà déclaré le 26 septembre 2006[6] qu'il considérait comme étant sa priorité de maintenir les droits européens de protection des données et a également souligné le manque de transparence des négociations avec l'UST.

B. FAITS ET CONTEXTE JURIDIQUE

B.1. SWIFT

SWIFT est une société coopérative de droit belge à responsabilité limitée établie à La Hulpe (Belgique). SWIFT fournit à ses clients – des institutions financières – des services automatisés standardisés ("messaging services") et des logiciels d'interface en vue de la transmission de messages financiers entre des institutions financières dans le monde entier. SWIFT n'est donc pas elle-même une banque ou une autre forme d'institution financière.
Environ 7.800 institutions financières y sont affiliées. SWIFT n'a pas d'exclusivité pour sa prestation de service. Les institutions financières peuvent faire effectuer leurs transactions de paiements par d'autres prestataires et d'autres moyens (VPN providers (fournisseurs de réseaux virtuels privés), Internet, fax, réseaux de banques, VISA, etc.). Outre des bureaux de vente dans différents pays, SWIFT dispose de deux centres de traitement (OC), établis en tant qu'agences ("branches") de SWIFT, une en Europe et une aux Etats-Unis. Dans ces OC, en tant que partie du service SWIFTNet FIN, tous les messages traités par SWIFT sont stockés, en miroir, pendant 124 jours afin de pouvoir faire office de "back-up recovery tool" en cas de contestation entre les institutions financières ou en cas de perte des données d'un client. Une fois passé ce délai, les données sont effacées.

B.1.1. *Description du flux de données et données traitées via le service SWIFTNet FIN*

Le flux de données effectué par SWIFT dans le cadre du service SWIFTNet FIN concerne l'envoi de messages relatifs à des transactions financières entre des institutions financières. Il convient de remarquer que SWIFT n'a par conséquent que des contacts avec des clients professionnels et n'entretient pas de relation contractuelle directe avec des clients (personnes physiques) d'institutions financières qui demanderaient ou recevraient une transaction financière sur ou via leurs comptes.
SWIFT ne fournit en outre ses services qu'à des institutions financières qui ont signé au préalable un cadre contractuel. Ce cadre contractuel est connu des institutions financières qui utilisent le service SWIFTNet FIN et se compose entre autres des prescriptions SWIFT ("by-laws"), des conditions générales, de la documentation spécifique relative au service (reprises intégralement dans le "manuel d'utilisateur de SWIFT" ou "SWIFT User

[5] Au sein du groupe de protection des personnes concernant le traitement de données à caractère personnel, établi sur la base de l'article 29 de la Directive 95/46/CE, ci-après le "Groupe 29".
[6] Voir le communiqué de presse publié http://ec.europa.eu/justice_home/fsj/privacy/news/docs/PR_Swift_Affair_26_09_06_en.pdf.

Handbook") et de la politique de SWIFT en matière de collecte des données ("data retrieval policy"). Il est complété par la "politique de compliance"[7] de SWIFT.

Les messages envoyés électroniquement peuvent être comparés à une "enveloppe" et à une "lettre", où "l'enveloppe" ou l'en-tête du message concerne des informations sur l'expéditeur, son code BIC[8], une identification de la banque réceptrice et enfin la date et l'heure du message. La "lettre" (contenu de l'enveloppe), donc le message en lui-même, est cryptée au moyen du cryptage PKI et contient des informations intégrées au moyen de champs standardisés. S'il s'agit d'un message concernant un paiement d'un client d'une banque[9], ces informations contiennent au minimum le montant de la transaction, la devise, la date valeur, le nom du bénéficiaire, l'institution financière du bénéficiaire, le client qui a demandé la transaction financière et l'institution financière de ce client. Les messages relatifs aux paiements peuvent toutefois contenir également d'autres informations comme des numéros de référence pour les paiements et (pour certains types de messages) du "texte non structuré" ("free format").

Le trajet d'un message de paiement international envoyé par l'intermédiaire du service SWIFTNet FIN se déroule comme suit (la première et la quatrième étape sont effectuées en dehors du fonctionnement de SWIFT) :

1. un ordre de paiement individuel d'un client donneur d'ordre (un individu ou une entreprise) est envoyé à sa banque (la "banque d'origine"). A moins que la banque d'origine ou le client donneur d'ordre ne choisisse une solution ou un service alternatif à SWIFT, la banque d'origine rédige un message SWIFT standardisé et crypté ;
2. la banque d'origine envoie le message SWIFT standardisé au moyen du service SWIFTNet FIN, ou choisit une solution ou un moyen alternatif à SWIFT. Soit le message est envoyé à la banque de correspondance à l'étranger, soit il est envoyé directement à la banque du bénéficiaire (si la banque d'origine a une relation de correspondance directe avec la banque du bénéficiaire) ;
3. la banque de correspondance envoie le même message via le réseau SWIFT à la banque du bénéficiaire ;
4. la banque du bénéficiaire informe le bénéficiaire que son paiement a été reçu et crédite son compte.

SWIFT agit à cet égard comme le porteur du message standardisé dans l'enveloppe fermée. Le service de messagerie comprend, au niveau des centres de traitement, une validation formelle du contenu, notamment la présence ou le contenu correct des données dans les champs prévus (par exemple, la banque de destination est-elle mentionnée? la devise est-elle précisée ? etc.). Cela requiert un décryptage momentané du contenu du message, y compris en ce qui concerne les données à caractère personnel. Ce décryptage a lieu de manière automatisée. En tant que partie du service de messagerie, les messages sont également conservés dans les centres de traitement en Europe et aux Etats-Unis pour la période susmentionnée de 124 jours.

---

[7] La déclaration de SWIFT concernant la "compliance" est disponible sur son site Internet www.swift.com.

[8] Le "BIC" (Bank Identifier Code) est un code international d'identification (parfois également appelé code swift) permettant de reconnaître chaque banque individuelle.

[9] Un transfert par un client est une des neuf catégories de messages SWIFT.

B.2. Sommations ("subpoenas")

Depuis les attentats de septembre 2001, l'UST a adressé plusieurs sommations au centre de traitement de SWIFT aux Etats-Unis. Après demande de renseignements, SWIFT a déclaré que, jusqu'à ce jour, elle avait reçu et accepté 64 sommations de l'UST suite aux attentats du 11 septembre 2001.

Avant 2001, SWIFT avait également fait l'objet de quelques sommations judiciaires ou administratives, mais SWIFT n'y a pas donné suite, en raison du délai (après 124 jours), ou parce que SWIFT pouvait avancer que les autorités pouvaient obtenir les données plus facilement auprès de la banque émettrice ou réceptrice, ou parce que SWIFT ne dispose pas d'outil de recherche dans ses centres de traitement pour faire une recherche sur la base du nom dans le centre de traitement.

Les sommations de l'UST sont d'un caractère totalement différent et peuvent être qualifiées de demandes **non individualisées et massives (technique "Rasterfandung" ou "carpetsweeping")** dans une première phase (voir ci-après). Le champ d'application des sommations est tant matériel que territorial et très large dans le temps et est défini dans les sommations et dans la correspondance de négociation entre l'UST et SWIFT.

Les sommations ont été appliquées pour toutes les transactions qui ont ou peuvent avoir un rapport avec le terrorisme, concernant x pays et juridictions, à cette date ou de … à … variant d'une à plusieurs semaines, dans et/ou en dehors des Etats-Unis, …). Il s'agit donc tant de messages sur des transactions interbancaires au sein des Etats-Unis, vers ou depuis les Etats-Unis, qu'en dehors des Etats-Unis, comme par exemple dans l'Union européenne.

Il ressort en outre des informations communiquées que l'UST part, dans ses sommations, d'une **définition** large **du "terrorisme"** comme étant "la lutte contre des attentats de terroristes contre les Etats-Unis qui ont eu lieu après le 11 septembre 2001 et un réseau global de cellules terroristes qui constitueraient un risque de violence accrue contre les ressortissants, les propriétés et les intérêts américains et les intérêts nationaux et étrangers". Il ressort ensuite des négociations que SWIFT a convenu avec l'UST d'une deuxième définition (conventionnelle) du terrorisme, énoncée comme suit : "une activité qui (i) implique un acte de violence ou un acte dangereux pour la vie humaine, la propriété ou l'infrastructure ; et (ii) semble viser (A) à intimider ou exercer une contrainte sur une population civile ; (B) influencer la politique d'un gouvernement par intimidation ou contrainte ou (C) influencer le comportement d'un gouvernement par une destruction de masse, des assassinats, des kidnappings ou l'enlèvement d'otages. Ceci inclut, de manière non limitative, des activités déployées par des organisations terroristes connues, mais exclut des activités de gouvernements reconnus".[10] La Commission observe que la référence aux Etats-Unis a été abandonnée dans cette définition conventionnelle.

Il ressort des vérifications de la Commission qu'une distinction **a été faite**, dans le processus d'extraction, **entre deux étapes**. D'une part, la conservation dans une boîte noire des messages fournis en vertu des sommations et d'autre part, la consultation effective de messages dans la boîte noire par l'UST sur la base de recherches. Ces deux étapes sont décrites ci-après.

Tous **les messages soumis aux sommations** ("subpoened messages") sont fournis par le centre de traitement de SWIFT aux Etats-Unis à l'UST et conservés dans une dite **boîte**

[10] "an activity that (i) involves a violent act or an act dangerous to human life, property, or infrastructure; and (ii) appears to be intended (A) to intimidate or coerce a civilian population; (B) to influence the policy of a government by intimidation or coercion; or (C) to affect the conduct of a government by mass destruction, assassination, kidnapping, or hostage-taking. This includes, but is not limited to, activities engaged in by known terrorist organizations, but excludes activities of recognized governments."

noire ("black box" ou "production database") qui est conservée dans les installations de l'UST.

Dans cette boîte noire, a lieu un décryptage automatique, au moyen d'un outil (logiciel de recherche) élaboré par l'UST et propriété de ce dernier, après quoi l'UST peut effectuer des recherches par nom. Ce logiciel de recherche, qui n'est pas disponible pour SWIFT, vérifie si certains noms de suspects définis au préalable apparaissent dans les messages[11]. SWIFT et l'UST ont convenu à cet égard que l'UST ne peut effectuer que des demandes ciblées qui sont liées à des enquêtes ponctuelles sur des activités terroristes.

Après demande formelle à cet égard par la Commission, SWIFT ne lui a fourni aucun chiffre précis quant au nombre de messages qui se trouveraient dans la boîte noire. Elle a justifié cela en affirmant que l'UST avait jugé que ces informations étaient importantes pour la sécurité nationale. Il a également été communiqué que ces informations ne pouvaient être divulguées que par l'UST, après application de la procédure de sécurité adéquate pour des fonctionnaires belges ayant une habilitation de sécurité adéquate.

Cependant, on peut déduire du champ d'application général des sommations et du volume moyen de messages traités quotidiennement par le service SWIFTNet FIN que le nombre de messages soumis aux sommations et qui se trouvent dans la boîte noire doit être très élevé. Dans une lettre du 14 septembre 2006, SWIFT a confirmé que l'UST "a parfaitement le droit, en vertu du droit américain, de soumettre la section américaine de SWIFT à une sommation afin que soient communiqués tous les messages SWIFT". Cela signifie donc que, rien que pour 2005, un total de 2.518.290.000 messages SWIFTNet Fin peut être soumis aux sommations[12].

B.3. <u>Réaction de SWIFT aux sommations</u>

SWIFT a obtenu de l'UST un certain nombre de garanties et de mécanismes de protection dont les principes ont été formellement documentés dans une correspondance entre SWIFT et l'UST.

B.3.1. *Négociations avec l'UST*

SWIFT a décidé de ne pas attaquer les sommations, prononcées à l'encontre de "l'agence" SWIFT aux Etats-Unis et non à l'encontre de SWIFT SCRL, devant un tribunal américain, mais bien de négocier directement avec l'UST afin d'obtenir des garanties claires. SWIFT souligne qu'elle a obtenu un niveau de protection unique dans ces négociations continues pour les données transférées pars ses soins.

Pour autant que la Commission ait pu le vérifier à l'aide des documents soumis, les premières conventions documentées concernaient la désignation d'un auditeur externe (Booz, Allen & Hamilton) et les caractéristiques du processus d'audit à compter du mois d'août 2002. SWIFT a obtenu le 15 septembre 2003 une "comfort letter" de l'UST, par laquelle l'UST manifestait son soutien à SWIFT au cas où des tiers comme des autorités d'autres pays mettraient en cause le respect des sommations de l'UST. A compter du 14 avril 2004, un certain nombre de garanties importantes ont été répertoriées, dont quelques-unes avaient été négociées dès le début du processus. Elles concernaient la définition conventionnelle du terrorisme et les critères de recherche et de collecte au 27 février 2004, et des conventions quant à la confidentialité maximale des données collectées, le contrôle de SWIFT sur les critères de recherche et sur la collecte. SWIFT a

[11] Comme confirmé par l'UST à SWIFT le 1er août 2002.

[12] Chiffre mentionné dans la même lettre de SWIFT du 14 septembre 2006. On peut également partir d'une circulation de messages normale moyenne journalière via SWIFTNet FIN se situant entre 6,9 millions (2005) et 11 millions de messages par jour (début 2006) et qui peut être soumise intégralement aux sommations.

également obtenu la garantie que la source originale des informations (SWIFT) serait tenue secrète par l'UST.

En résumé, les garanties, telles que convenues entre l'UST et SWIFT, concernent ce qui suit :

- l'UST n'a pas accès au système SWIFT lui-même et aux données qui y sont enregistrées ;
- seules les données relatives à des enquêtes sur le terrorisme peuvent être demandées ;
- les recherches dans la boîte noire ne sont possibles que sur la base de dossiers d'enquête spécifiques et ciblés concernant des activités terroristes ;
- un audit permanent par l'auditeur américain Booz, Allen & Hamilton a été prévu à partir de la mi-2002. Cet audit concerne des audits end-to-end du système de l'UST afin de fournir à SWIFT des garanties supplémentaires que le système était sûr (vérifier la conformité avec les normes internationales ISO pour la sécurité des informations), que les finalités étaient limitées aux enquêtes sur le terrorisme, que les scrutinizers (voir ci-après) avaient accès à toutes les informations faisant l'objet des recherches des analystes de l'UST et afin d'apporter des améliorations continues au système ;
- deux employés de SWIFT ("scrutinizers") ont reçu une habilitation de sécurité afin d'être présents lors de l'extraction des données par l'UST. Ils vérifient, pour chaque extraction de l'UST, la légitimation sur une base régulière, initialement par la prise d'un échantillon statistique ("statistical sampling"), ensuite au niveau 100 %. Ils ne font rapport au management de SWIFT qu'en ce qui concerne le respect des principes d'extraction, pas sur le détail d'extractions spécifiques ;
- la boîte noire de l'UST reste soumise au contrôle des "scrutinizers" au moyen d'un accès 24h/24, d'un monitoring en temps réel et d'une possibilité de blocage des recherches, même à partir du moment où la boîte noire a été placée dans un local physiquement protégé des autorités américaines ;
- si l'UST cherchait un mandat judiciaire pour contraindre SWIFT à respecter une sommation, l'UST serait d'accord de ne pas invoquer comme précédent le respect par SWIFT des sommations, ou de s'y fier, procédé par lequel SWIFT s'est réservé tous les droits de défense en cas d'une telle action ;
- la possibilité a été prévue pour SWIFT de récupérer dans la boîte noire tous les messages non collectés de l'UST, fut-ce avec l'obligation de conserver ces données tant que la possibilité existe qu'une sommation soit prononcée quant à ces données ;
- des normes de confidentialité strictes sont fixées.

B.3.2. *Information aux Autorités de contrôle*

Au départ, seule la validité juridique des sommations était vérifiée par le conseiller général de SWIFT et des conseillers externes. Les décisions relatives au respect des sommations étaient prises par le président-directeur (CEO) de SWIFT, le comité de direction ("Board of Directors") et le comité d'audit ("Audit and Finance Committee ou "AFC"). Le comité de direction a reçu une brève explication sur la sommation de la part du président du comité d'audit. En mars 2002, une présentation a été faite à ce sujet au comité de direction et une discussion a eu lieu. Un rapport est depuis dressé de façon périodique.

SWIFT a également informé le "Senior level oversight Group" (G-10), dont la Banque nationale de Belgique. Par lettre du 10 août 2006, la Commission a interrogé la Banque nationale de Belgique ("BNB") sur ses compétences de surveillance. Dans une réponse du 29 août 2006, celle-ci a confirmé que "la BNB, en sa qualité de "overseer", a été informée par SWIFT en février 2002 de l'existence d'une sommation américaine à l'encontre de l'agence de SWIFT aux Etats-Unis."

La BNB estime ne pas être compétente pour apprécier le respect par SWIFT des sommations successives de l'UST. Ce point de vue est également partagé par le G-10.

C. APPLICABILITE DE LA LVP

Il y a lieu de vérifier si la LVP s'applique à SWIFT en sa qualité d'exploitant du système SWIFTNet FIN et ce en tant que "responsable du traitement" ou en tant que "sous-traitant".

C.1. Champ d'application territorial

La LVP "*est applicable au traitement de données à caractère personnel lorsque le traitement est effectué dans le cadre des activités réelles et effectives d'un établissement fixe du responsable du traitement sur le territoire belge (…)*" (article 3bis, 1° de la LVP).

Le siège social et le siège décisionnel de SWIFT sont établis en Belgique et la société a un numéro d'entreprise belge, étant le 413330856. Il ne fait dès lors aucun doute qu'il s'agit bien d' "*activités réelles et effectives*" et d'"*un établissement fixe sur le territoire belge*", indépendamment de la question de savoir si SWIFT est le responsable[13] du traitement, question qui sera traitée ci-après.

SWIFT a fait référence au fait que le centre de traitement aux Etats-Unis n'a nullement une personnalité juridique distincte et qu'il n'est pas du tout question de communiquer des données à une société externe en dehors de l'Union européenne (dans le cadre du traitement interne normal du service SWIFTNet FIN).

Du point de vue du droit des sociétés, SWIFT conclut sur cette base que le traitement a toujours été soumis aux règles auxquelles la société belge est assujettie, parce que le centre de traitement pourrait juridiquement être identifié à SWIFT SCRL. Elle en déduit que la protection en vertu du droit belge s'applique également à son centre de traitement aux Etats-Unis. Bien que SWIFT ait utilisé cet argument du droit des sociétés afin de mettre en cause l'application des articles 21 et 22 de la LVP (voir infra), la Commission fait remarquer que cet argument peut aussi confirmer que le traitement de données à caractère personnel est soumis au droit belge, y compris à la LVP.

C.2. Champ d'application matériel

Il ressort clairement de la description du flux de données et des données traitées via le service SWIFTNet FIN (voir supra à la rubrique B.1.) qu'il est question d'un "traitement" de "données à caractère personnel" au sens de l'article 1, §§1 et 2 de la LVP. Les messages financiers qui sont traités[14] et enregistrés dans le cadre du service SWIFTNet FIN contiennent en effet des données de personnes physiques telles que l'identité du bénéficiaire et l'identité du donneur d'ordre de services financiers tels que les ordres de paiement.

Enfin, on peut signaler que l'article 10.10 des conditions générales de SWIFT prévoit l'applicabilité du droit belge aux dispositions et conditions relatives à la fourniture et à l'utilisation des services et produits SWIFT. Il faut bien entendu y inclure le droit belge en matière de protection des données à caractère personnel et la LVP.

[13] Pour l'analyse concernant la responsabilité de SWIFT, voir ci-après.

[14] En vertu de l'article 1, § 2 de la LVP, toute collecte, extraction, consultation, utilisation, communication par transmission, diffusion ou toute autre forme de mise à disposition, ainsi que l'interconnexion de données à caractère personnel constituent un traitement.

D. APPRECIATION QUANT A SAVOIR SI SWIFT, LES INSTITUTIONS FINANCIERES ET LA BANQUE NATIONALE DE BELGIQUE SONT RESPONSABLES DU TRAITEMENT OU SOUS TRAITANTS

Pour répondre à la demande du Collège du renseignement et de la sécurité, il importe de vérifier le rôle de SWIFT, des clients de SWIFT (dénommés ci-après "institutions financières") et de la Banque nationale de Belgique à la lumière de la LVP.

La question est de savoir si SWIFT, les institutions financières ou la Banque nationale de Belgique doivent être qualifiés de responsables du traitement ou de sous-traitants. La responsabilité du respect de la LVP est en principe imposée au responsable du traitement. L'article 1, § 4 de la LVP définit le responsable du traitement comme "*(…) la personne morale (…) qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel.*" Le sous-traitant est par contre la "*personne physique ou morale, l'association de fait ou l'administration publique qui traite des données à caractère personnel pour le compte du responsable du traitement et est autre que la personne qui, placée sous l'autorité directe du responsable du traitement, est habilitée à traiter les données*". La distinction entre les deux qualifications a des conséquences très importantes en ce qui concerne le respect de la LVP : le sous-traitant a en principe une responsabilité plus limitée au regard de la LVP et les personnes concernées ne peuvent en principe exercer leurs droits qu'auprès du responsable.

La définition légale à l'article 1, § 4 de la LVP est **impérative** et l'on ne peut y déroger par des conventions contractuelles.

Pour déterminer qui est responsable, la LVP prévoit essentiellement un **critère fonctionnel**. La question est en d'autres termes de savoir qui avait une "emprise" sur le traitement de données à caractère personnel via le service SWIFTNet FIN ou qui pouvait prendre de facto les décisions cruciales relatives à la finalité et aux moyens des traitements. Des critères formels, comme la définition contractuelle des services ou la qualité des parties contractantes, sont à cet égard utiles mais a priori non déterminants.

Pour apprécier correctement une qualification possible des acteurs précités, il convient également de garder à l'esprit quelles finalités et donc quels traitements sont visés. La Commission estime nécessaire d'opérer une distinction entre les traitements suivants : d'une part, assurer le fonctionnement du service SWIFTNet FIN et d'autre part, effectuer des ordres de paiement internationaux faisant appel au service SWIFTNet FIN.

D.1. <u>Le traitement de données à caractère personnel dans le cadre du service SWIFTNet FIN</u>

SWIFT a systématiquement affirmé qu'elle n'était pas responsable du traitement pour le service de messagerie, mais seulement un sous-traitant. Dans les contacts avec la Commission, SWIFT s'est basée à cet égard sur un certain nombre d'arguments qui peuvent être résumés comme suit :

- SWIFT se compare à un prestataire de service postal de télécommunications ou de courrier électronique dont on estime normalement qu'il n'est pas responsable de traitement mais seulement un sous-traitant[15] ;

[15] Le considérant 47 de la Directive 95/46/CE dispose que "*lorsqu'un message contenant des données à caractère personnel est transmis via un service de télécommunications ou de courrier électronique dont le seul objet est de transmettre des messages de ce type, c'est la personne dont émane le message, et non celle qui offre le service de transmission, qui sera normalement considérée comme responsable du traitement de données à caractère personnel contenues dans le message ; que, toutefois, les personnes qui offrent ces services seront normalement considérées comme responsables du traitement des données à caractère personnel supplémentaires nécessaires au fonctionnement du service ;*"

- SWIFT affirme que, dans les conventions contractuelles avec les institutions financières[16], la qualification de SWIFT en tant que sous-traitant a été établie ;
- SWIFT avance qu'elle dispose, en tant que sous-traitant, d'une "marge de manœuvre normale" pour déterminer l'organisation de son service, notamment au niveau des mesures techniques et organisationnelles nécessaires pour effectuer le traitement ;
- SWIFT affirme qu'elle offre ses services dans un environnement "business to business", elle n'entretient pas de contact direct et n'a pas non plus de relation contractuelle avec les clients des institutions financières, parmi lesquels des personnes physiques ;
- SWIFT affirme enfin qu'elle n'a pas élaboré ou développé de capacité de recherche afin de rechercher des données à caractère personnel qui seraient éventuellement mentionnées dans les messages qu'elle traite.

Vu la définition fonctionnelle du responsable en vertu de la LVP, la Commission estime que le **contexte au sein duquel le traitement est effectué** (celui d'une société coopérative à responsabilité limitée) et la **connaissance de la position exacte des institutions financières et de la direction de la SCRL SWIFT** sont cruciaux pour procéder à une qualification exacte concernant le traitement normal de données au sein du service SWIFTNet FIN.

La comparaison de la SCRL SWIFT avec un prestataire normal de service postal de télécommunications ou de courrier électronique est un argument formel et semble insuffisante. Cette comparaison formelle implique en effet que la SCRL SWIFT aurait une position comparable à celle de toute entreprise de télécommunications quelconque qui peut proposer au niveau international un VPN pour l'échange de messages financiers. En réalité, il apparaît que SWIFT utilise toutefois un modèle de fonctionnement et de services plus complexe qui part d'un **réseau coopératif international à forte gestion centrale** à l'égard des 7800 institutions financières qui utilisent le service. L'exploitation et les modalités de fonctionnement de tels réseaux diffèrent fondamentalement du simple concept de services où un seul prestataire professionnel traite des données à caractère personnel à l'égard d'une autre partie professionnelle ou non. L'appréciation de la qualification "responsable" ou "sous-traitant" est, dans ce contexte, délicate. En cas de cumul de différents acteurs, le rôle et les responsables de chaque entité doivent en effet être déterminés clairement.

Le traitement normal au sein du service SWIFTNet FIN semble à première vue assez obscur de par son caractère international et non transparent. La structure des réseaux coopératifs (internationaux) n'est toutefois pas unique et connaît deux précédents clairs.

- Ainsi, pour des listes négatives de commerçants VISA et Mastercard, exploitées au niveau international, le Groupe 29 a déjà admis que, pour l'exploitation de réseaux coopératifs internationaux, une coresponsabilité des institutions financières et des opérateurs de banques de données (VISA, Mastercard) semble recommandée[17]. Les opérateurs de banques de données n'ont à cet égard aucun contact direct avec les personnes concernées et ne sont en principe actifs que dans un environnement "business to business", bien que leurs services soient distribués dans le circuit "retail" via leurs parties contractantes.

[16] Voir article 4.5.3 des conditions générales de SWIFT qui concerne "les obligations en matière de protection des données" ("Data Protection Obligations"). Dans sa documentation contractuelle, SWIFT opère une distinction entre d'une part le traitement de données à caractère personnel obtenues des institutions financières lors de la souscription ou de l'utilisation des services de SWIFT et d'autre part les données à caractère personnel traitées dans les messages ou fichiers par les institutions financières via les services ou produits SWIFT. En ce qui concerne ce dernier traitement, il a été explicitement établi que les institutions financières sont censées être responsables du traitement ("data controller").

[17] Voir le paragraphe 16 des Guidelines for Terminated Merchant Databases du 11 janvier 2005 qui dispose ce qui suit : "The development and operation of a terminated merchant database require the joint action of two Participants acting as joint data controllers for any particular set of personal data relating to a specific merchant, namely 1) the Database Operator, and 2) the Participant that has a contractual relationship with the merchant."

- La structure pyramidale des systèmes de réservation automatisés existants dans le domaine des transports aériens (Computer Reservation System ou "CRS") constitue un deuxième précédent. A cet égard, les agences de voyage et les compagnies aériennes (entre autres) introduisent des données à caractère personnel dans les systèmes de réservation, les entreprises nationales de distribution offrent un accès au système de réservation contre une indemnité (frais de réservation) et enfin la gestion centrale du système de réservation est assurée au niveau le plus élevé. La Commission[18] et l'autorité de protection des données française, la CNIL[19], ont déjà défendu ici le point de vue de la responsabilité conjointe.

Pour les réseaux coopératifs précités, les autorités de protection des données partent donc, surtout ces dernières années, d'une coresponsabilité des utilisateurs professionnels de la banque de données et du gestionnaire de la base de données.

Maintenant que le contexte dans lequel le traitement est effectué a été précisé, il reste la question de savoir si et dans quelle mesure SWIFT et/ou les institutions financières ont défini la finalité et les moyens du service SWIFTNet FIN. SWIFT est un coresponsable pour autant que, avec d'autres (les institutions financières), c'est-à-dire conjointement, elle détermine la finalité et les moyens des traitements.

- Le service de SWIFT n'est **pas un simple service de transport** et ne peut être réduit à l'exécution d'une mission pour quelqu'un d'autre qui déterminerait entièrement cette mission. La réalité est que la direction de SWIFT, plus que les institutions financières, détermine les modalités de livraison des services au moyen de **contrats d'affiliation et de standards techniques qui sont en grande partie établis**. Par ailleurs, si chaque institution financière individuelle souhaitait et pouvait mettre en œuvre un certain format ou une adaptation de la protection des données, il est clair que le traitement standardisé de SWIFT pourrait être compromis. Ceci n'empêche toutefois pas que, si un nombre critique de demandes (SWIFT parlait d'une "demande du marché") d'adaptation du service ou de développement d'un nouveau service survenait, SWIFT adapterait ses services en étroite concertation avec ses membres. Un exemple concret de la possibilité susmentionnée réside dans le fait que les informations traitées dans le cadre du service SWIFTNet FIN ont déjà été adaptées suite à la demande de la Financial Action Task Force ("FATF/GAFI") et après consultation des institutions financières, afin d'accroître les possibilités d'identification des personnes physiques[20].

- SWIFT n'est pas un sous-traitant du fait qu'elle peut prendre des décisions quant à la finalité et aux moyens des traitements, **décisions qui vont d'ailleurs plus loin que "l'espace de manœuvre" normal défini légalement dans lequel un sous-traitant normal peut décider** lors de l'exercice des missions qui lui sont confiées. Du fait que SWIFT poursuit des finalités propres dans le cadre des opérations du service SWIFTNet FIN, elle est justement en mesure d'offrir une valeur ajoutée par rapport au service fourni par ses concurrents, parmi lesquels ses propres clients. Une illustration de la valeur ajoutée offerte par SWIFT concerne le **décryptage automatique des données dans les centres de traitement par lequel SWIFT opère une vérification formelle quant au contenu de chaque message** afin de vérifier le contenu correct des champs prévus. En outre, seule la direction de SWIFT décide de l'installation des

---

[18] Voir la recommandation n° 01/98 de la Commission relative au "Système de réservation automatisé" du 14 décembre 1998.

[19] La Commission souligne ici l'exemple des systèmes de réservation automatisés qui existent dans le secteur aérien et qui comprennent d'une part des clients comme les compagnies aériennes et les agences de voyage et d'autre part les exploitants de ces systèmes de réservation comme Galileo. Les responsabilités des deux acteurs ont déjà été commentées au nom de la CNIL le 11 septembre 1996, à l'occasion de la 18e Conférence internationale de protection de la vie privée et des données nominatives. Voir le texte sur le site de la DPA canadienne : http://www.privcom.gc.ca/speech/archive/02_05_a_960918_03_f.asp

[20] D'après rapport

centres de traitement et de la distribution des services via l'établissement de ses bureaux de vente. SWIFT dispose enfin d'une grande autonomie quant à l'imposition de sa politique de protection des données aux institutions financières, concernant des **éléments qui tombent en dehors des obligations normales d'un sous-traitant et d'un contrat de sous-traitant** (voir article 16, § 1 de la LVP). Par exemple, la "politique de compliance" ("no comment policy") diffère de la politique de certains clients (européens) de SWIFT et des clauses relatives à la vie privée qui figurent dans les différents contrats d'affiliation de SWIFT pour le service SWIFTNet FIN. Les exemples précités concernent les aspects juridiques essentiels effectifs du traitement au sujet desquels seul le responsable a voix au chapitre et non le sous-traitant.

- Il n'est **pas inhabituel que les responsables du traitement n'aient pas de contact direct avec les personnes concernées** et la LVP n'exige pas non plus cet élément pour parler d'un responsable. Autrement dit, l'application de la LVP n'est absolument pas exclue dans un contexte "business to business". Des exemples concrets de tels responsables qui n'ont pas de contact direct ou de relation contractuelle avec la personne concernée ont déjà été mentionnés précédemment (VISA, Mastercard, entreprises de distribution et Computer Reservation Systems ou "CRS").

- Si l'on prétendait enfin que seules les 7800 institutions financières seraient responsables des traitements des données à caractère personnel via le service SWIFTNet FIN, cela impliquerait que le justiciable serait confronté à une si grande **dispersion et à un si grand fractionnement juridique des responsables concernés**, que cela les empêcherait de facto d'exercer leurs droits résultant de la LVP.

- Enfin, SWIFT n'est pas un sous-traitant parce qu'**il n'appartient pas au sous-traitant de prendre, d'initiative et sans information et accord du responsable, des décisions cruciales pendant (presque) 5 ans au sujet de la réception de données** par des administrations telles que l'UST. SWIFT a toutefois clairement pris toutes les décisions cruciales au sujet de la communication de données à l'UST, et l'a fait à l'insu de ses 7800 clients. C'est ce qu'il ressort des éléments suivants :

    1. Le rôle déterminant de SWIFT lors de la communication de données à l'UST ressort des négociations continues et secrètes avec l'UST et des conventions qui ont été conclues dans ce cadre à partir de fin 2001. L'application concrète des sommations a été négociée en secret par SWIFT par la mise en place du système de "boîte noire", et contrôlée plus tard via la définition des critères de recherche et d'extraction, le processus d'audit et les scrutinizers (voir supra). SWIFT a également obtenu la garantie que les informations quant à la source resteraient confidentielles.

    2. Depuis le siège belge, les décisions cruciales ont été prises et suivies concernant la communication des données à l'UST. Il s'agissait de la décision d'examiner la légalité de la sommation américaine d'octobre-novembre 2001 et d'y consentir, de la première décision de procéder à la transmission, opérée d'un commun accord entre le conseiller général, le président-directeur et le chef de l'audit et de la délégation, au comité d'audit par le comité de direction, dans le cadre de la vérification du processus d'extraction. Les 7800 clients de SWIFT n'ont pas été informés des décisions secrètes de SWIFT qui avaient été prises en concertation avec l'UST.

    3. Il apparaît que les clients de SWIFT ne sont pas informés de l'ampleur concrète et des modalités de la transmission de données à l'UST. Cette approche repose sur

la "no comment policy" de la politique de compliance[21] que la direction de SWIFT a établie depuis 1993.

4. Enfin, suite aux communiqués de presse de juin 2006, les clients de SWIFT n'étaient pas en mesure d'arrêter la communication à l'UST. Après les communiqués de presse relatifs aux sommations, un organisme de crédit autrichien[22] a demandé à SWIFT de cesser de communiquer des données à l'UST. SWIFT a refusé d'accéder à cette demande de son client par lettre du 9 août 2006, affirmant que sa section américaine était soumise à la juridiction des Etats-Unis et qu'elle devait respecter les sommations à condition qu'elles soient valables et contraignantes en vertu du droit américain.

Sur la base des considérations précitées, la Commission conclut que SWIFT est un responsable au sens de la LVP pour les traitements effectués via le service SWIFTNet FIN. L'on examinera ci-après s'il est également question d'une coresponsabilité, pour autant que SWIFT détermine conjointement avec les institutions financières la finalité et les moyens des traitements.

D.2. L'exécution d'ordres de paiement internationaux au moyen du service SWIFTNet FIN

La question se pose ensuite de savoir si les institutions financières ont également déterminé la finalité et les moyens du traitement de sorte qu'elles sont coresponsables au sens de la LVP.

Une fois encore, il est important de garder à l'esprit le contexte dans lequel les institutions financières communiquent des données à caractère personnel à SWIFT. **Les institutions financières interviennent en principe à un autre niveau, à savoir le niveau du traitement d'ordres de paiement.** Ce traitement diffère de l'échange des *messages financiers* qui, sur le plan "business to business" (généralement interbancaire), est effectué par SWIFT. L'échange de messages financiers présente bien entendu un lien pratique avec les ordres de paiement. L'échange et le stockage de données s'avèrent justement *nécessaires, suite à l'ordre de paiement, afin de traiter la transaction correctement et sûrement dans la circulation interbancaire*. Le traitement de SWIFT ne se passe pas "au guichet", en contact direct avec l'intéressé qui donne l'instruction d'effectuer un ordre de paiement. Il a lieu, au contraire, dans le contexte du "back office" des institutions financières où des applications comme le scannage des ordres de paiement et la réalisation d'opérations interbancaires sont en principe effectués conformément aux standards et aux usages professionnels de chaque institution financière, aux usages du secteur et aux normes existantes. La Commission conclut que les traitements "réalisation d'ordres de paiement" et "échange de messages de paiement" sont souvent liés dans la pratique, bien qu'il s'agisse d'opérations différentes dont les finalités et donc les traitements ne peuvent pas être assimilés.

SWIFT a affirmé que les institutions financières sont responsables de la réalisation du traitement qui consiste à traiter des ordres de paiement internationaux. Les institutions financières qui font appel au service SWIFTNet FIN ne sont en effet pas des sous-traitants de SWIFT pour ce traitement, étant donné qu'elles n'agissent nullement à ce niveau pour le compte de SWIFT.

[21] La déclaration de SWIFT en matière de compliance est disponible sur son site Internet www.swift.com.
[22] La Niederoesterreichische Landesbank – Hypothekenbank AG, Kremsergasse 20 à 3100 St.-Pölten, Autriche

Il est également important de garder à l'esprit que les institutions financières sont autonomes et qu'elles peuvent poursuivre leurs propres objectifs au niveau interbancaire. La Commission constate que les institutions financières prennent souvent des décisions cruciales dans la circulation interbancaire quant à la communication de données à caractère personnel à SWIFT, souvent à l'insu de leurs clients. C'est ce qu'il ressort des éléments suivants :

- Les institutions financières **décident souvent de manière autonome, dans la circulation interbancaire, des moyens mis en œuvre pour le traitement d'un ordre de paiement donné.** Elles ont le choix d'utiliser ou non le service de SWIFT pour l'envoi de messages financiers relatifs à des transactions individuelles. Elles peuvent, au besoin, utiliser ou développer des services alternatifs ou concurrents pour l'envoi de ces messages financiers dans la circulation interbancaire (e-mail, fax, téléphone,…) à une banque de correspondance,… Les choix à ce niveau détermineront les caractéristiques globales en matière de vie privée concernant les ordres de paiement que l'institution financière traite. Etant donné la diversité des services au niveau interbancaire, les institutions financières sont libres, quant au choix du service interbancaire, de se laisser guider par des éléments tels que la politique de protection de la vie privée du prestataire professionnel, outre la protection des informations qui est bien entendu toujours requise. Les institutions financières peuvent utiliser, à titre de garantie, une forte politique de protection de la vie privée d'un certain prestataire ou une certaine solution comme un VPN, afin de garantir au maximum leurs services et la confiance de leurs clients.

- Les institutions financières **connaissent le cadre contractuel du service SWIFTNet FIN**. Il ressort de la documentation contractuelle (Data Retrieval Policy[23]) et de la politique de SWIFT en matière de compliance que les clients de SWIFT **étaient au courant du principe général de communication de données à caractère personnel suite à des sommations adressées à eux-mêmes ou à SWIFT**. SWIFT a avancé[24] que le nombre de sommations adressées aux institutions financières serait de l'ordre de milliers voire même de dizaines de milliers par an. On peut donc douter du fait que les institutions financières actives sur le marché des paiements internationaux ne seraient pas au courant du principe général des sommations.

- Les institutions financières doivent, en tant que prestataires professionnels, **pouvoir évaluer les éventuels risques (relatifs à la vie privée) et les implications pour le client concerné qui seraient liés au service SWIFTNet FIN**, auquel elles souscrivent en tant que prestataire professionnel. Il est important, à cet égard, de vérifier si la politique de protection de la vie privée de l'institution donneuse d'ordre contient des dispositions claires quant à ces risques.

- Vu leur contact direct avec les donneurs d'ordre pour les instructions de paiement, les institutions financières jouent un **"rôle de guichet" essentiel**. La Commission n'exclut pas que les institutions financières soient considérées comme "intermédiaires" pour l'exercice des droits des personnes concernées dans le cadre du service SWIFTNet FIN, pour autant que cela se fasse au moyen d'un accord clair avec SWIFT en tant que responsable du traitement dans le cadre du service SWIFTNet FIN.

---

[23] Qui dispose ce qui suit :"Afin d'exclure tout doute, rien dans ce document de politique ou, plus généralement, dans les obligations de confidentialité de SWIFT à l'égard de ses clients ne sera considéré comme un obstacle pour SWIFT pour extraire, utiliser ou communiquer des données relatives à la circulation ou des données issues de messages, pour autant que cela soit raisonnablement nécessaire afin de respecter une sommation sérieuse ou une autre procédure légale par un tribunal ou une autre autorité compétente ("For the avoidance of any doubt, nothing in this policy or, more generally, SWIFT's obligations of confidence to customers, shall be construed as preventing SWIFT from retrieving, using, or disclosing traffic or message data as reasonably necessary to comply with a bona fide subpoena or other lawful process by a court or other competent authority.")

[24] En réaction à un rapport d'une réunion avec la Commission du 22 août 2006.

Etant donné les considérations qui précèdent, la Commission estime que les institutions financières actives dans la circulation des paiements internationaux sur le plan "business to business" (interbancaire) peuvent également déterminer la finalité et les moyens des traitements qui leur sont confiés (le traitement d'ordres de paiement de leurs clients). Dans la mesure où le service SWIFTNet FIN est utilisé, elles peuvent, conjointement avec SWIFT, être considérées comme coresponsables du traitement.

D.3. Responsabilité de la Banque nationale de Belgique

Par un projet de résolution commun du 5 juillet 2006, le Parlement européen a exprimé le souhait à l'égard des Etats membres[25] de "*vérifier et de veiller qu'il n'existe pas de vide juridique au niveau national et que la législation communautaire en matière de protection des données s'applique également aux banques centrales*". Il a dès lors été demandé aux Etats membres de transmettre les résultats de cette vérification à la Commission européenne, au Conseil et au Parlement européen.

La Commission établit que la BNB, en tant que "overseer", n'a déterminé ni la finalité, ni les moyens du traitement de données à caractère personnel via le service SWIFTNet FIN. La BNB ne peut dès lors pas être responsable au sens de la LVP en ce qui concerne le traitement précité. La BNB, en tant que "overseer", a bien été informée par SWIFT en février 2002 de l'existence d'une sommation américaine.

Etant donné le projet de résolution précité, la Commission a souhaité vérifier auprès de la BNB, en tant que "overseer", le contenu concret de l' "oversight", et dans quelle mesure la BNB considère comme étant sa tâche de veiller à ce que SWIFT ait suffisamment couvert les risques juridiques tels que les risques en matière de protection de la vie privée. La BNB a répondu ce qui suit dans une lettre du 28 août 2006 :
"*(…) En vertu de l'article 8 de sa Loi organique*[26]*, la BNB veille au bon fonctionnement des systèmes de compensation et de paiements. Cette mission se rapporte aux tâches du Système européen de banques centrales (SEBC), en particulier l'article 22 des statuts du SEBC. Cette mission très spécifique des banques centrales est connue sous le terme* "*oversight*"*. Cette activité est exercée dans une perspective de système, où le bon fonctionnement du système global de compensation ou de paiement occupe une position centrale afin de garantir la stabilité financière et d'éviter lesdits* "*risques système*" *avec un effet domino de faillites bancaires (…)*" Elle ajoute que :
"*La Banque (…), en sa qualité de* "*overseer*"*, n'a aucune responsabilité pour les actes de SWIFT. L'approbation ou la désapprobation des décisions opérationnelles, financières, juridiques ou concernant le droit des sociétés du management n'est pas demandée à la Banque par SWIFT et n'est pas non plus obtenue.*" et "*(…) que les banques centrales du G-10 se sont concertées dans le courant de 2002 concernant l'affaire des sommations américaines et sont arrivées à la conclusion que ces sommations ne relevaient pas de l'* "*oversight*" *des banques centrales. Aucun nouvel élément n'a ensuite été fourni, obligeant le Senior Level Oversight Group à revoir cette conclusion.*"
[Traduction réalisée par le secrétariat de la Commission, en l'absence d'une traduction officielle].

Il ressort des éléments précités que le respect de la LVP par SWIFT n'est pour l'instant pas considéré comme faisant partie de l' "oversight" individuel et coopératif.

---

[25] Projet de résolution commun sur l'interception de données de virements bancaires du système SWIFT par les services secrets américains.
[26] Loi du 22 février 1998 *fixant le statut organique de la Banque Nationale de Belgique*.

Dans la mesure où la BNB intervient toutefois *en tant que client de SWIFT* et confierait à cet égard des données à caractère personnel au service SWIFTNet FIN, elle pourrait être considérée comme responsable comme mentionné à la rubrique D.2.

E. EXAMEN DES ÉVENTUELLES VIOLATIONS DE LA LVP

La demande d'avis concerne la question des éventuelles violations de la LVP par SWIFT. La question de savoir si les institutions financières (belges) ont violé la LVP ne fait pas partie au sens strict de l'objet de l'avis et n'a pas pu être examinée vu le temps limité dont a disposé la Commission. Etant donné que la Commission estime cependant qu'il est question de coresponsabilité dans le chef des institutions financières, elle se tient à disposition pour apprécier ultérieurement les éventuelles violations par des institutions financières (belges) individuelles.

La Commission souligne qu'il existe des différences fondamentales entre l'Union européenne et les Etats-Unis en ce qui concerne les législations et les principes régissant les traitements de données à caractère personnel. Les traitements de données à caractère personnel sont caractérisés, dans le droit européen, par le haut niveau de protection établi en Europe en vertu des conventions applicables comme l'article 8 de la CEDH, la Convention n° 108[27] et les directives européennes applicables telles que la Directive 95/46/CE.

La Commission souligne **un certain nombre de malentendus – fréquents – qui existent parfois au sujet des notions de "protection adéquate" et de "respect de la norme ou de la loi (relative à la protection de la vie privée)".** Elle souligne, pour l'interprétation de ces notions, **qu'il ne suffit pas uniquement de procéder à un contrôle par un auditeur externe, de respecter des standards ou normes techniques et de prévoir des mesures de sécurité technique adéquates**. Les principes applicables de la LVP vont bien plus loin.

L'on examinera donc ci-après si SWIFT a respecté tous les principes applicables de la LVP, même si elle a déjà atteint un haut degré de protection des données. Lors de l'évaluation, une distinction a été faite entre la question de savoir si, d'une part, des infractions à la LVP ont été commises dans le cadre du fonctionnement normal du service SWIFTNet FIN et si, d'autre part, des infractions à la LVP ont été commises dans le cadre du transfert des données à l'UST.

E.1. SWIFT a-t-elle commis des infractions à la LVP dans le cadre du fonctionnement normal du service SWIFTNet FIN ?

E.1.1. *Base légale (article 5 b) de la LVP et article 7 b) de la Directive 95/46/CE)*

Sur la base de l'article 5 de la LVP, les données à caractère personnel des donneurs d'ordre ou des bénéficiaires ne peuvent être traitées que dans un nombre limité de cas. Le traitement de données à caractère personnel dans le cadre du fonctionnement normal du service SWIFTNet FIN semble légitime dans la mesure où il est nécessaire à l'exécution du contrat entre SWIFT et l'organisme de crédit concerné (article 5 b) de la LVP et article 7 b) de la Directive 95/46/CE).

---

[27] Convention du 28 janvier 1981 *pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, M.B., 30 décembre 1993, approuvée par la loi du 17 juin 1991 *portant approbation de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, faite à Strasbourg le 28 janvier 1981*.

E.1.2. *Obligation d'information (article 9 de la LVP et article 11 de la Directive 95/46/CE)*

Dans la mesure où SWIFT est responsable du traitement, elle est également soumise à l'obligation d'information des personnes concernées. Cela signifie entre autres que les personnes physiques dont les données ont été échangées dans les messages de paiement devaient au moins être informées conformément à l'article 9 de la LVP. Les personnes concernées devaient par exemple savoir qui pouvaient être les destinataires des données qu'elles transmettaient à leur organisme de crédit (SWIFT, autorités,…) et pour quelles finalités leurs données pouvaient être traitées.

Etant donné que SWIFT collecte les données à caractère personnel au moyen d'ordres des institutions financières, elle n'obtient pas directement les données à caractère personnel des personnes concernées. Dans ce cas, il importe, selon l'article 9, § 2 de la LVP (article 11 de la Directive 95/46/CE), "*dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, au plus tard au moment de la première communication des données,* [de] *fournir à la personne concernée au moins les informations*[28], *sauf si la personne concernée en avait déjà été informée*" par les institutions financières. Cela signifie que, si SWIFT n'a pas veillé à ce que les institutions financières aient informé les personnes concernées conformément à l'article 9, § 1 de la LVP et qu'aucune exception spécifique n'a été prévue à l'obligation d'information dans l'arrêté d'exécution de la LVP, SWIFT a commis une infraction à l'article 9, § 2 de la LVP.

Enfin, le fait que SWIFT n'entretienne pas de relation directe avec les personnes concernées ne peut nullement être considéré comme une raison suffisante pour ne pas respecter l'obligation d'information, par exemple via les institutions financières. Bien que la LVP ne prescrive pas la manière concrète dont les informations doivent être données, on peut tenir compte du contexte dans lequel les données sont traitées, à condition que la technique d'information choisie vise à informer effectivement et clairement les personnes concernées. La Commission a déjà estimé, dans le cadre de l'avis n° 48/2003 du 18 décembre 2003 *concernant la transmission de données à caractère personnel par certaines compagnies aériennes vers les Etats-Unis,* que "*le mode de communication au client n'est pas suffisamment explicite, les informations étant intégrées dans le texte des conditions générales de transport, communiquées sur demande ou via Internet*". La Commission[29] a cependant estimé, dans un contexte de manifestations de masse telles que les matches de football, que les informations pouvaient avoir lieu individuellement (sur les tickets d'accès) ou collectivement (en plaçant par exemple des panneaux clairs et visibles à l'entrée du stade).

Vu sa coresponsabilité à la lumière de la LVP, SWIFT ne s'est pas concertée suffisamment avec les institutions financières afin de respecter l'obligation d'information (article 9 de la LVP). Ceci a donné lieu à une information insuffisante à l'égard des personnes concernées et au non-respect de l'article 9 de la LVP.

[28] Selon l'article 9, § 2 de la LVP, les informations pertinentes sont "*le nom et l'adresse du responsable, les finalités du traitement (…) et d'autres informations supplémentaires, notamment les catégories de données concernées et les destinataires ou les catégories de destinataires, l'existence d'un droit d'accès et de rectification des données la concernant, sauf dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont traitées, ces informations supplémentaires ne sont pas nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données ;*"

[29] Avis n° 10/2005 du 15 juin 2005.

E.1.3. *Obligation de déclaration (article 17 de la LVP et article 21 de la Directive 95/46/CE)*

Etant donné que SWIFT est responsable du traitement, elle est en principe soumise à l'obligation de déclaration du traitement qui permet une transparence et un contrôle généraux, fussent-ils minimaux. La Commission constate cependant que SWIFT n'a pas fait de déclaration pour le traitement de données à caractère personnel dans le cadre du service SWIFTNet FIN, contrairement aux autres traitements tels que l'administration propre du personnel de SWIFT qui n'entrent pas dans le cadre du présent avis.

La Commission estime dès lors que **l'article 17 de la LVP n'a pas été respecté.**

E.1.4. *Transfert de données à caractère personnel vers un pays ne présentant pas un niveau de protection adéquat (articles 21 et 22 de la LVP et articles 25 et 26 de la Directive 95/46/CE)*

SWIFT devait tenir compte de la réglementation sur la transmission de données à caractère personnel vers des pays tiers. Les dispositions de la Directive 95/46/CE (chapitre IV, articles 25 et 26) régissent cette problématique et ont été repris partiellement dans la LVP, plus précisément aux articles 21 et 22 de la LVP.

SWIFT a communiqué à la Commission qu'elle estimait que l'exigence d'un niveau de protection adéquat découlant de l'article 21 de la LVP ne s'appliquait pas au traitement dans le cadre de son service SWIFTNet FIN. En résumé, elle avance les arguments suivants à cet égard :

- L'interdiction de transfert de données (article 21, § 1) ne serait pas valable étant donné que le transfert n'a pas été effectué depuis la Belgique par la société mère.
- L'interdiction de transfert de données ne serait pas valable étant donné que le transfert n'a pas été effectué vers une société tierce et étant donné que, selon une règle du droit des sociétés, la succursale (centre de traitement aux Etats-Unis) de SWIFT sans personnalité juridique relèverait toujours, juridiquement parlant, de la société mère. Cette unité juridique impliquerait que, dans le cadre du service SWIFTNet FIN, le traitement reste toujours soumis à un niveau de protection adéquat, à savoir le droit belge.
- Subsidiairement, pour autant que les exceptions légales de l'article 22, § 1 de la LVP soient bien d'application, SWIFT avance que le transfert serait nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable (article 22, 2° de la LVP), soit que le transfert serait nécessaire à l'exécution d'un contrat dans l'intérêt de la personne concernée (article 22, 3° de la LVP), soit que le transfert serait nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important (article 22, 4° de la LVP).
- Le transfert a lieu dans un environnement fortement sécurisé avec un cryptage du contenu des messages.

Les articles 21 et 22 de la LVP sont d'application dès qu'il est question de soumettre des données à caractère personnel à un transfert vers un pays ne présentant pas un niveau de protection adéquat tel que les Etats-Unis. La LVP utilise de nouveau à cet égard un **critère fonctionnel**. Etant donné que les articles 21 et 22 de la LVP sont précisés de manière fonctionnelle et constituent un droit contraignant d'ordre public, les règles du droit des sociétés peuvent difficilement réduire à néant l'ensemble du régime de protection en vertu de la Directive 95/46/CE.

La Commission constate que, dans le cadre du fonctionnement normal du service SWIFTNet FIN, il est question d'un transfert de messages européens vers des centres de traitement en Europe et aux Etats-Unis. Le fait que les données soient envoyées à une filiale ne constitue pas un critère selon la LVP pour ne pas appliquer les conditions de la loi.

Ce transfert a lieu quotidiennement et massivement (11 millions de messages par jour début 2006). Après transfert aux centres de traitement, les données sont soumises à l'ensemble des opérations[30] qui sont propres au service SWIFTNet FIN.

La Commission observe qu'une protection poussée ou un cryptage de données à caractère personnel n'empêche pas que le transfert de données codées soit toujours soumis aux articles 21 et 22 de la LVP.

La Commission estime par ailleurs que les exceptions prévues à l'article 22 de la LVP ne peuvent être invoquées pour le traitement via le service SWIFTNet FIN. Etant donné les alternatives et les services concurrents qui existent sur le marché des paiements internationaux, un recours au service SWIFTNet FIN peut encore difficilement être considéré comme nécessaire pour toute institution financière pour effectuer un ordre de paiement.

Enfin, la notion de "motif d'intérêt public important" doit toujours être interprétée dans l'ordre juridique belge, conformément aux normes juridiques valables en Belgique comme l'article 8 de la CEDH. SWIFT a avancé que le placement en miroir des centres de traitement est considéré comme un élément critique pour le système financier mondial. Elle affirme que le placement en miroir lui a été imposé par les "overseers" (banques centrales du G-10) pour des raisons de sécurité et de fiabilité, étant donné que l'infrastructure de SWIFT est considérée comme critique pour l'industrie financière globale. Au niveau européen, il a cependant déjà été jugé que les Etats-Unis n'offraient pas un niveau de protection adéquat à la lumière de la Directive 95/46/CE. Même si le fonctionnement du système financier mondial devait avoir un impact sur l'ordre public en Belgique, ce n'est toutefois pas une justification suffisante à la lumière de la Directive 95/46/CE pour installer un centre de traitement aux Etats-Unis sans niveau de protection adéquat.

Etant donné que les Etats-Unis ne tombent pas dans la catégorie des pays présentant un niveau de protection adéquat, les principes de la "sphère de sécurité" ("Safe Harbour") ont été élaborés spécifiquement pour les Etats-Unis, sur décision de la Commission européenne[31]. En ce qui concerne tous les pays qui ne garantissent pas un niveau de protection adéquat comme les Etats-Unis, la Commission européenne a en outre prévu des dispositions contractuelles adéquates, conformément à l'article 26, 2 de la Directive 95/46/CE[32]. Il existe enfin le système des "Binding Corporate Rules", c'est-à-dire les règles d'entreprise contraignantes, qui peut permettre le transfert de données à caractère personnel vers des pays tiers, sans niveau de protection adéquat. **La Commission estime que le système des règles d'entreprise contraignantes ("binding corporate rules"), conformément à l'article 26, 2 de la Directive 95/46/CE, est une mesure adéquate et requise pour prévoir les garanties adéquates pour les transferts de données quotidiens et massifs effectués via les centres de traitement d'une entreprise multinationale telle que SWIFT.** Un tel code de conduite doit toutefois être autorisé en Belgique par le Roi, après avis de la Commission.

La Commission estime que la protection que **SWIFT** a prévue pour le traitement des données dans le cadre de son centre de traitement aux Etats-Unis **ne satisfait pas aux articles 21 et 22 de la LVP (articles 25 et 26 de la Directive 95/46/CE).**

---

[30] Notamment le décryptage automatique et la vérification formelle des données.

[31] Voir la Décision 2000/520/CE de la Commission du 26 juillet 2000 conformément à la Directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la "sphère de sécurité" et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique (notifiée sous le numéro C(2000) 2441)

[32] Voir à ce sujet : http://europa.eu.int/comm/justice_home/fsj/privacy/modelcontracts/index_en.htm

E.2. SWIFT a-t-elle violé la LVP lors du transfert de données à l'UST ?

La Commission souhaite vérifier ci-après si SWIFT a violé la LVP dans le cadre de la communication de données à caractère personnel à l'UST.

E.2.1. *Base légale (article 5 de la LVP, article 7 b) de la Directive 95/46/CE et article 8 de la CEDH)*

La Commission insiste sur le fait qu'elle ne met pas en cause la légalité ou le caractère contraignant de la législation américaine et des sommations américaines, ce qui relève clairement de la compétence de l'autorité américaine. Par contre, elle peut examiner si l'exécution des sommations américaines peut trouver, dans le droit belge sur le traitement de données à caractère personnel, une base de légitimation. En vertu de l'article 5 de la LVP, les données à caractère personnel des donneurs d'ordre ou des bénéficiaires ne peuvent être traitées que dans un nombre limité de cas. SWIFT n'invoque pas formellement une base légale en vertu du droit belge et a uniquement fait référence aux sommations américaines dont elle affirme avoir examiné la légalité et le caractère contraignant. Toutefois, prima facie, surtout l'article 5 c) (obligation légale du responsable) et 5 f) (réalisation d'un intérêt important et légitime du responsable) semblent pertinents pour pouvoir légitimer la communication de données à caractère personnel à l'UST.

En ce qui concerne l'article 5 c), la Commission souscrit à l'avis du Groupe 29 du 1er février 2006 concernant la législation Sarabanes-Oxley[33]. Le Groupe 29 a déjà affirmé qu' "*Une obligation imposée par une loi ou un règlement étrangers qui exigeraient l'établissement de systèmes de signalement ne saurait être qualifiée d'obligation légale légitimant le traitement des données dans l'UE. Toute autre interprétation permettrait à des législations étrangères de contourner les règles fixées par l'UE avec la directive 95/46/CE.*". Ceci signifie par conséquent que les sommations américaines ne peuvent pas être considérées comme une base légitimant le traitement de données, conformément à l'article 5 c) de la LVP.

Rejoignant le point de vue de la Commission de la vie privée française (la CNIL) dans le dossier SOX[34], la Commission estime qu'il est impossible, dans le cas des sommations américaines, de nier l'intérêt légitime de SWIFT au sens de l'article 5 f) de la LVP. En d'autres termes, on ne peut contester que SWIFT a un intérêt légitime à se soumettre à une sommation valable et exécutable en vertu du droit américain. En cas de non respect par SWIFT de ces sommations, SWIFT court en effet le risque de se voir infliger des sanctions civiles en vertu du droit américain. La Commission pense dès lors que le transfert de données à l'UST **repose sur un intérêt légitime et important dans le chef de SWIFT au sens de l'article 5 f) de la LVP**.

[33] Voir l'avis 1/2006 *relatif à l'application des règles européennes de protection des données aux dispositifs internes d'alerte professionnelle ("whistleblowing") dans les domaines bancaire, de la comptabilité, du contrôle interne des comptes, de l'audit, de la lutte contre la corruption et les infractions financières.*

[34] CNIL, Document d'orientation adopté par la Commission le 10 novembre 2005 pour la mise en œuvre de dispositifs d'alerte professionnelle conformes à la loi du 6 janvier 1978 modifiée en août 2004, relative à l'informatique, aux fichiers et aux libertés.

Néanmoins, SWIFT aurait dû réaliser que **les mesures exceptionnelles en vertu du droit américain pouvaient difficilement légitimer une violation cachée, systématique, massive et de longue durée des principes européens fondamentaux en matière de protection des données.** Ce principe de base se retrouve au deuxième alinéa de l'article 8 de la CEDH[35]. Les exigences de base strictes en vertu de cet article ont déjà été expliquées à plusieurs reprises par la Cour européenne des Droits de l'homme, notamment au moment de confronter des activités secrètes de surveillance à des critères tels que l'exigence de prévisibilité de la norme et l'exigence de mesures de contrôle suffisantes et effectives[36].

E.2.2. *Principe de proportionnalité (article 4, § 1, 3° de la LVP) et délai de conservation (article 4, § 1, 5° de la LVP)*

La Commission estime qu'en l'espèce, il semble s'agir d'un "conflict of laws" entre le droit américain et le droit belge, qui a forcé SWIFT à faire des choix difficiles après la réception des sommations américaines. A la lumière du principe de proportionnalité, il est toutefois essentiel de vérifier si SWIFT **a également recherché un équilibre entre les deux systèmes juridiques et a, pour ce faire, suffisamment examiné et appliqué la possibilité d'alternatives en vertu du droit belge ou européen.** Le fait que SWIFT soit soumise aux sommations et ait entretenu activement des négociations confidentielles avec l'UST sur l'application des sommations n'empêche pas en effet que le traitement doive être effectué en conformité avec les principes du droit belge et du droit européen.

Vu le principe de nécessité, on se demande **quelles alternatives SWIFT avait une fois qu'il était établi qu'elle était soumise à des sommations valables et contraignantes.** Un certain nombre d'options semblaient exister, à savoir :

- Contester les sommations imposées en vertu du droit américain.

  A la question de savoir pourquoi les sommations n'ont pas été soumises aux juges aux Etats-Unis, SWIFT a répondu que les premières sommations avaient été introduites juste après les événements de septembre 2001. Les sommations reposeraient actuellement sur une base légale en vertu du droit américain (codifiée dans ledit "Patriot Act"[37]). SWIFT a en outre affirmé qu'il y avait un risque que le juge américain décide d'ordonner à SWIFT de communiquer toutes les données sans limites.

- Appliquer les procédures officielles et les traités en matière de collaboration judiciaire.

  Les recommandations et procédures qui existent pour une collaboration judiciaire sur le plan international et européen et qui sont visées pour la prévention et la lutte contre le financement du terrorisme via un accès à des données au sein d'institutions financières ne semblent pas suivies.

---

[35] Formulé comme suit : "*Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.*"

[36] Voir l'affaire Rotaru contre Roumanie (§ 55 et suivants) qui fait référence à des affaires antérieures telles que Malone contre Royaume-Uni du 2 août 1984, Series A n° 82, p. 32, § 67, et *Amann* contre *Suisse* [GC], n° 27798/95, § 65, Cour européenne des Droits de l'homme 2000-II, § 56).

[37] Le USA PATRIOT Act (Public Law 107-56) ou, en toutes letters, le Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, est une proposition de loi américaine (H.R. 3162) qui a été adoptée à la majorité en 2003 par le Congrès américain. La loi a pour but d'offrir plus de possibilités à l'autorité américaine de réunir des informations et d'intervenir en cas de terrorisme potentiel (source : http://nl.wikipedia.org).

On peut faire référence à cet égard aux recommandations publiques de la FATF ("GAFI")[38]. La FATF est un organe intergouvernemental créé en 1989 ayant pour but de développer et de promouvoir des mesures de politique nationales et internationales afin de lutter contre le blanchiment et le financement du terrorisme. La recommandation n° 40 de la FATF comporte la disposition selon laquelle "*Les pays devraient mettre en place des contrôles et des garanties pour faire en sorte que les informations échangées par les autorités compétentes ne soient utilisées que de la manière autorisée et en conformité avec leurs obligations de protection de la vie privée et de protection des données.*"[39]

On peut en outre se référer à la collaboration dans le cadre du "Groupe d'Egmont"[40]. Par l'intermédiaire de ce groupe informel, un échange de renseignements financiers est actuellement mis en place via les cellules nationales opérationnelles de renseignements financiers ("financial intelligence units" ou "FIU") des 101 pays dont la Belgique et les Etats-Unis. Cet échange est réalisé via le "Egmont Secure Web" ou "ESW".

Les organes et systèmes alternatifs précités pourraient offrir, à la lumière de la Directive 95/46/CE, des garanties complémentaires lors de l'échange d'informations en matière de blanchiment et de financement du terrorisme. Enfin, on peut signaler que, à la suite des attentats du 11 septembre 2001, deux accords[41] internationaux ont été négociés entre l'Union européenne et les Etats-Unis. Ceux-ci ont été signés le 25 juin 2003 mais sont en attente d'être ratifiés par les deux parties. En vertu de l'article 18 de la Convention de Vienne sur le droit des traités[42], *un Etat doit s'abstenir d'actes qui priveraient un traité de son objet et de son but lorsqu'il a signé le traité ou a échangé les instruments constituant le traité sous réserve de ratification, tant qu'il n'a pas manifesté son intention de ne pas devenir partie au traité*.

La Commission constate cependant que **SWIFT s'est limitée au respect du droit américain et à la recherche de solutions via des négociations secrètes avec l'UST**. La Commission regrette que les alternatives susmentionnées n'aient pas été envisagées et que les autorités[43] européennes compétentes en matière de protection des données n'aient pas été consultées afin de confronter le transfert massif de données à caractère personnel à l'UST au regard du droit européen.

En ce qui concerne l'application du principe de proportionnalité, la Commission fait remarquer que le transfert massif, caché, durant depuis des années et systématique de données à caractère personnel peut également être considéré comme une violation de l'article 4, § 1, 3° de la LVP.

Enfin, le contrôle du délai de conservation des données dans la boîte noire doit également être jugé essentiel à la lumière du respect du principe de proportionnalité. Une distinction est établie entre le délai de conservation normal qui est d'usage dans le cadre du fonctionnement normal des centres de traitement de SWIFT et les délais de conservation

---

[38] Publiées sur le site http://www.fatf-gafi.org. Voir http://www.fatf-gafi.org/dataoecd/42/43/33628117.PDF concernant les 40 recommandations.

[39] "*Countries should establish controls and safeguards to ensure that information exchanged by competent authorities is used only in an authorised manner, consistent with their obligations concerning privacy and data protection.*"

[40] Zie http://www.egmontgroup.org/about_egmont.pdf

[41] "Agreement on extradition between the EU and the US" et l' "Agreement on mutual legal assistance between the EU and the US". Voir les publications sur http://eur-lex.europa.eu/LexUriServ/site/en/oj/2003/l_181/l_18120030719en00270033.pdf et http://europa.eu.int/eur-ex/pri/en/oj/dat/2003/l_181/l_18120030719en00340042.pdf#search=%22Agreement%20on%20mutual%20legal%20assistance%20between%20the%20european%20union%22

[42] Convention de Vienne sur le droit des traités, 23 mai 1969, M.B. du 25 décembre 1993, entrée en vigueur : le 1er octobre 1992. Les Etats-Unis ont signé ce traité.

[43] Compte tenu de l'analyse des "overseers" qui se sont déjà déclarés incompétents en 2002 en matière de sommations.

qui sont d'application pour les données dans la boîte noire mise à la disposition de l'UST[44]. Après vérification des accords entre SWIFT et l'UST, il s'avère qu'il semble être question d'un **délai de conservation d'une durée indéterminée**, donc excédant largement le délai de conservation normal dans le cadre du service SWIFTNet FIN, ce qui est contraire au principe de proportionnalité. Initialement, il existait la possibilité de conserver les messages dans la boîte noire aussi longtemps qu'ils représentaient une utilité éventuelle pour une recherche. Ensuite, SWIFT a eu la possibilité de récupérer de l'UST tous les messages non collectés, fut-ce avec l'obligation de conserver ces données tant que la possibilité existe qu'une sommation soit prononcée quant à ces données (voir supra au point B.4.1). La Commission constate que cette "possibilité de déplacement" de données (de la boîte noire vers SWIFT) a peu d'influence sur le délai de conservation à proprement parler, qui reste en principe indéterminé, c'est-à-dire aussi longtemps qu'existe la possibilité d'une sommation concernant ces données. La Commission signale enfin que pour le moment, aucune vérification indépendante effective n'a pu être réalisée concernant le délai concret de conservation de données dans des cas individuels. Par conséquent, on ne peut exclure que des données à caractère personnel puissent être conservées dans la boîte noire durant des années sans vérification indépendante.

Sur la base des considérations susmentionnées, la Commission estime que la pratique susmentionnée d'un transfert massif, caché, durant depuis des années et systématique de données à caractère personnel à l'UST avec un délai de conservation d'une durée indéterminée **constitue une violation des principes de proportionnalité et du délai de conservation limité tel que formulé aux articles 4, § 1, 3° de la LVP (proportionnalité) et 4, § 1, 5° de la LVP (délai de conservation), à la suite des articles 6.1. (c) et 6.1. (e) de la Directive 95/46/CE. En tant que responsable, SWIFT aurait dû se rendre compte que ces principes étaient jugés fondamentaux dans l'ordre juridique européen.**

E.2.3. *Principe de finalité*

La Commission insiste sur le fait qu'elle reconnaît l'intérêt et la légitimité de la lutte mondiale contre le terrorisme. Toutefois, à la lumière de la LVP, il est crucial de savoir si les sommations, compte tenu de leur formulation, pouvaient en effet uniquement être utilisées pour la lutte contre le terrorisme et n'impliquaient pas, par exemple, une autorisation pour d'autres finalités, tel que suggéré dans certains média[45]. Cet aspect dépend de la définition et de la communication de la finalité du traitement via l'obligation d'information, qui sera expliquée ci-après.

Cependant, il ne relève pas de la compétence de la Commission de mettre en cause la légitimité des sommations américaines.

E.2.4. *Obligation d'information dans le chef de SWIFT (articles 4, § 1, 2° et 9, § 2 de la LVP et article 8 de la CEDH)*

La Commission établit que tout contrôle de la finalité dépend entièrement de la transparence requise et de la définition précise des finalités du traitement. Elle fait remarquer à ce sujet que :

- La finalité exacte du traitement (combattre le terrorisme) a en principe été imposée et définie dans les sommations dont la finalité exacte a toujours été traitée avec la plus grande confidentialité et de façon non-transparente ;

[44] Les délais de conservation que l'UST utiliserait pour les données qu'elle a réunies après extraction de la boîte noire ne sont pas connus.
[45] Voir par exemple un article dans le Knack du 9 août 2006 dans lequel l'auteur suggère qu'il serait question d'affaires qui n'auraient aucun rapport avec le terrorisme comme "une affaire liée à la drogue".

- Les finalités qui ont été formulées dans les communications de SWIFT au grand public avant le 23 juin 2006 (et donc aux personnes concernées) restaient très vagues et aucun lien clair n'a été mentionné avec le terrorisme (mention d'"activités illégales" et "comportement illégal" dans la politique publique de compliance de SWIFT) ;
- Ce n'est que dans les communiqués de presse généraux diffusés après le 23 juin 2006 qu'il a été précisé à plusieurs reprises que SWIFT ne communiquait les données que pour "des recherches spécifiques au terrorisme" (dans la déclaration relative à la compliance du 23 juin 2006 et les mises à jour de cette déclaration après cette date).

La Commission constate en outre que la politique "sans commentaire" de SWIFT en matière de compliance semble en contradiction avec l'exigence de transparence qui découle de la Directive 95/46/CE et du deuxième alinéa de l'article 8 de la CEDH. Cette politique semble inspirée en grande partie des obligations strictes de confidentialité imposées à SWIFT dans le cadre de recherches individuelles de l'UST, par les règles générales de confidentialité et le devoir de discrétion en vigueur dans le monde des services financiers et enfin par les intérêts commerciaux et le risque au niveau de la réputation de SWIFT.

Il faut toutefois se poser la question délicate de savoir **où doit être trouvé l'équilibre entre le haut degré de confidentialité offert par SWIFT au système et l'ampleur des traitements à la suite des sommations et d'autre part les diverses obligations de transparence que SWIFT, en tant que responsable**, assume en vertu des articles 4, § 1, 2° de la LVP (exigence de la définition de la finalité dans la politique vie privée) et 9, § 2 de la LVP (obligation d'information). D'autre part, on se demande jusqu'à quel point SWIFT pouvait ET devait informer les institutions financières et les personnes concernées en vertu de l'article 9, § 2 de la LVP sur le transfert des données via l'UST.

La Commission est consciente que des obligations légales ou conventionnelles de confidentialité existent, aussi bien pour des sommations américaines que pour des sommations belges, ce qui implique que l'obligation normale d'information à l'égard de la personne physique concernée (suspect, qui fait l'objet de la sommation) ne sera pas toujours d'application lors de l'exécution d'une sommation.

Cependant, la Commission attire l'attention sur une différence fondamentale qui distingue les sommations de l'UST des sommations dans le droit belge. Sous la rubrique B.2., il a déjà été précisé que les sommations de l'UST doivent être qualifiées de **demandes non individualisées et massives (technique "Rasterfandung" "carpetsweeping")** qui fonctionnent en deux phases, ce qui diffère des sommations belges qui sont exercées *ab initio* par cas individuel. Il a également été remarqué à la fin de la rubrique B.2. que l'UST "a parfaitement le droit, en vertu du droit américain, de soumettre la section américaine de SWIFT à une sommation afin que soient communiqués tous les messages SWIFT". Cela signifie donc que, rien que pour 2005, un total de 2.518.290.000 messages SWIFTNet Fin peut être soumis aux sommations[46].

Vu le deuxième alinéa de l'article 8 de la CEDH, **les obligations de transparence subsistent au niveau collectif**, donc en ce qui concerne le phénomène des demandes de renseignements massives via des sommations européennes ou américaines.

Compte tenu du caractère secret, massif et inhabituel du transfert de données, la Commission estime dès lors que SWIFT devait au moins informer les institutions financières et les autorités de contrôle en matière de protection des données (autorités européennes, DPA dont la Commission) des sommations de l'UST.

---

[46] Chiffre mentionné dans la même lettre de SWIFT du 14 septembre 2006. On peut également partir d'une circulation de messages normale moyenne journalière via SWIFTNet FIN se situant entre 6,9 millions (2005) et 11 millions de messages par jour (début 2006) et qui peut être soumise intégralement aux sommations.

E.2.5. *Obligation de déclaration*

En vertu de l'article 17, § 6 de la LVP, une transmission de données à caractère personnel à l'étranger doit être déclarée. SWIFT a effectué cette déclaration pour une multitude d'autres traitements[47] mais pas pour le transfert de données à l'UST et encore moins pour la finalité de "compliance". Ceci est étrange, étant donné qu'il n'est pas inhabituel pour des institutions financières et d'autres prestataires de services financiers tels que SWIFT de déclarer leur finalité de "compliance" et leurs transferts internationaux séparément auprès de la Commission. Ainsi, les références à des traitements de "compliance" en vertu de la loi du 11 janvier 1993[48] sont assez courantes dans le chef des institutions financières responsables.

En ne mentionnant pas dans la déclaration les transferts de données aux Etats-Unis et la finalité de compliance dans le cadre des sommations, **SWIFT a violé l'article 17, § 1 de la LVP**.

E.2.6. *Exigence d'un contrôle indépendant du transfert de données (article 28 de la Directive 95/46/CE et article 8 de la CEDH)*

Seule la direction de SWIFT semblait au courant des modalités du transfert à l'UST[49] avant les communiqués de presse de juin 2006 en Belgique. Le contrôle indépendant requis en vertu de l'article 28 de la Directive 95/46/CE semble donc en grande partie empêché par le fait que les transferts massifs de données par SWIFT ont été traités avec la plus grande confidentialité. Ainsi, ni les institutions financières concernées, ni les autorités européennes compétentes en matière de protection des données n'ont été mises au courant du phénomène massif des sommations américaines.

L'exigence d'un contrôle indépendant découle toutefois également du deuxième alinéa de l'article 8 de la CEDH. Dans l'affaire Rotaru, la Cour européenne des Droits de l'homme a affirmé : "*La norme juridique implique, entre autres, qu'une ingérence de l'exécutif dans les droits de l'individu soit soumise à un contrôle efficace que doit normalement assurer, au moins en dernier ressort, le pouvoir judiciaire, car il offre les meilleures garanties d'indépendance, d'impartialité et de procédure régulière (…)*"[50].

En maintenant la surveillance massive et secrète à l'insu des autorités européennes compétentes en matière de protection des données et sans contrôle indépendant au sein des Etats-Unis (le seul contrôle a été mené par des sociétés du secteur privé, à savoir SWIFT et son auditeur), **il y a eu violation des exigences de l'article 28 de la Directive 95/46/CE.**

[47] Notamment la gestion des membres, la gestion de la clientèle, …

[48] *Loi relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme.*

[49] Indépendamment du fait que la BNB, en tant que "lead overseer", ait été informée de l'existence de la première sommation et que les institutions financières sont censées connaître la pratique des sommations et le fait que les transactions SWIFT devaient être soumises à ces sommations, selon les documents contractuels.

[50] "*The rule of law implies, inter alia, that interference by the executive authorities with an individual's rights should be subject to effective supervision, which should normally be carried out by the judiciary, at least in the last resort, since judicial control affords the best guarantees of independence, impartiality and a proper procedure (see the Klass and Others judgment cited above, pp. 25-26, § 55).*"

E.2.7. *Interdiction de transmission lors de transferts ultérieurs à des destinataires de données tels que l'UST (articles 21 de la LVP et 25 et 26 de la Directive 95/46/CE)*

A défaut de dispositions d'exception applicables au sens des articles 22 de la LVP et 26 de la Directive 95/46/CE (voir supra), la Commission insiste sur le fait que le transfert de données à l'UST ne peut nullement être régularisé de manière satisfaisante via la conclusion de "dispositions contractuelles" ou de "binding corporate rules" au sein du groupe SWIFT.

Tout comme dans le précédent PNR[51], pour ces transferts appelés ultérieurs ("onward transfers"), des accords spécifiques entre les Etats-Unis et l'Union européenne semblent être requis afin de s'assurer que le destinataire des données (l'UST) appliquera correctement des règles de protection adéquates conformément au droit européen. C'est le sens que donne le Groupe 29 aux articles 25 et 26 de la Directive 95/46/CE[52]. Pour SWIFT, le cadre des accords du GAFI aurait pu servir de point de départ, mais la question est de savoir pourquoi cette option n'a pas été choisie.

Vu le fait que le destinataire des données (l'UST) n'a jamais été soumis à un niveau de protection adéquat, conformément à l'article 21 de la LVP et à la Directive 95/46/CE, la Commission estime que SWIFT **a violé l'article 21, § 1 de la LVP**. Il peut être considéré comme une faute grave d'évaluation dans le chef de SWIFT de soumettre depuis des années, de manière secrète et systématique, une quantité massive de données à caractère personnel à la surveillance de l'UST sans avoir contacté en même temps les autorités européennes compétentes et la Commission afin de trouver une solution en vertu du droit belge et européen.

PAR CES MOTIFS,

sur la base de son examen général, la Commission estime que :

- la LVP s'applique à l'échange de données via le service SWIFTNet FIN ;

- SWIFT et les institutions financières sont conjointement responsables à la lumière de la LVP pour les traitements de données à caractère personnel via le service SWIFTNet FIN ;

- SWIFT est responsable du traitement de données à caractère personnel telles que traitées via le service SWIFTNet FIN ;

- les institutions financières sont responsables étant donné qu'elles déterminent également la finalité et les moyens de l'exécution des ordres de paiement dans la circulation interbancaire. Les institutions financières font procéder, notamment au niveau interbancaire, au traitement de messages financiers relatifs à ces messages de paiement via le service SWIFTNet Fin ;

[51] Depuis début janvier 2003, les Etats-Unis ont exigé un accès aux Passenger Name Records (les données de voyage et de réservation, ou "PNR") de tous les passagers sur des vols à destination, en provenance ou en transit aux Etats-Unis. Depuis lors, des solutions sont recherchées au niveau européen quant à l'exigence d'un niveau de protection adéquat lors du transfert de ces données aux USA.

[52] Voir le document de travail du 24 juillet 1998 du Groupe 29 concernant *le transfert de données personnelles vers des pays tiers : application des articles 25 et 26 de la directive relative à la protection des données*, publié sur http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/1998_en.htm

- en ce qui concerne le traitement normal de données à caractère personnel dans le cadre du service SWIFTNet FIN, SWIFT aurait dû respecter ses obligations en vertu de la LVP, dont l'obligation d'information, l'obligation de déclaration et l'obligation de prévoir un niveau de protection adéquat conformément à l'article 21, § 2 de la LVP ;

- en ce qui concerne la communication de données à caractère personnel à l'UST, la Commission estime que SWIFT se trouve en situation de conflit entre le droit américain et européen et a au minimum commis un certain nombre de fautes d'évaluation lors du traitement des sommations américaines. Qu'il convient notamment de considérer comme une grave erreur d'évaluation dans le chef de SWIFT le fait d'avoir soumis à une surveillance pendant des années une quantité massive de données à caractère personnel, ce secrètement et systématiquement, sans justification suffisante et claire et sans contrôle indépendant conformément au droit belge et européen. Dans ce contexte, SWIFT aurait dû, dès le début, être consciente du fait que, outre l'application du droit américain, les principes fondamentaux du droit européen doivent également être respectés, comme le principe de proportionnalité, le délai de conservation limité, la politique de transparence, l'exigence de contrôle indépendant et celle de niveau de protection adéquat. Ces exigences sont en effet exprimées dans le deuxième alinéa de l'article 8 de la CEDH, la Convention n° 108, la Directive 95/46/CE et la LVP et s'appliquent à SWIFT. La Commission se réfère également au précédent international dans le dossier PNR. Les autorités compétentes en matière de protection des données (la Commission, ses pairs et la Commission européenne) auraient du être informées dès le début, ce qui aurait pu permettre d'élaborer une solution au niveau européen pour la communication de données à caractère personnel à l'UST, en respectant les principes précités en vigueur dans le droit européen. A cet égard, le gouvernement belge aurait également pu être sollicité afin de requérir une initiative au niveau européen.

Vu la matière complexe et son importance, la Commission se tient à disposition pour fournir un avis ultérieur quant à cette problématique.

L'administrateur,	Vu l'empêchement du président, le vice-président,
(sé) Jo BARET	(sé) Willem DEBEUCKELAERE

A. INTRODUCTION ... 2
B. FAITS ET CONTEXTE JURIDIQUE ... 3
B.1. SWIFT ... 3
B.1.1. *Description du flux de données et données traitées via le service SWIFTNet FIN* ... 3
B.2. Sommations ("subpoenas") ... 5
B.3. Reactie van SWIFT op de dwangbevelen ... 6
B.3.1. *Négociations avec l'UST* ... 6
B.3.2. *Information aux Autorités de contrôle* ... 7
C. APPLICABILITE DE LA LVP ... 8
C.1. Champ d'application territorial ... 8
C.2. Champ d'application matériel ... 8
D. APPRECIATION QUANT A SAVOIR SI SWIFT, LES INSTITUTIONS FINANCIERES ET LA BANQUE NATIONALE DE BELGIQUE SONT RESPONSABLES DU TRAITEMENT OU SOUS TRAITANTS ... 9
D.1. Le traitement de données à caractère personnel dans le cadre du service SWIFTNet FIN . 9
D.2. L'exécution d'ordres de paiement internationaux au moyen du service SWIFTNet FIN 13
D.3. Responsabilité de la Banque nationale de Belgique ... 15
E. EXAMEN DES ÉVENTUELLES VIOLATIONS DE LA LVP ... 16
E.1. SWIFT a-t-elle commis des infractions à la LVP dans le cadre du fonctionnement normal du service SWIFTNet FIN ? ... 16
E.1.1. *Base légale (article 5 b) de la LVP et article 7 b) de la Directive 95/46/CE)* ... 16
E.1.2. *Obligation d'information (article 9 de la LVP et article 11 de la Directive 95/46/CE)* ... 17
E.1.3. *Obligation de déclaration (article 17 de la LVP et article 21 de la Directive 95/46/CE)* ... 18
E.1.4. *Transfert de données à caractère personnel vers un pays ne présentant pas un niveau de protection adéquat (articles 21 et 22 de la LVP et articles 25 et 26 de la Directive 95/46/CE)* 18
E.2. SWIFT a-t-elle violé la LVP lors du transfert de données à l'UST ? ... 20
E.2.1. *Base légale (article 5 de la LVP, article 7 b) de la Directive 95/46/CE et article 8 de la CEDH)* 20
E.2.2. *Principe de proportionnalité (article 4, § 1, 3° de la LVP) et délai de conservation (article 4, § 1, 5° de la LVP)* ... 21
E.2.3. *Principe de finalité* ... 23
E.2.4. *Obligation d'information dans le chef de SWIFT (articles 4, § 1, 2° et 9, § 2 de la LVP et article 8 de la CEDH)* ... 23
E.2.5. *Obligation de déclaration* ... 25
E.2.6. *Exigence d'un contrôle indépendant du transfert de données (article 28 de la Directive 95/46/CE et article 8 de la CEDH)* ... 25
E.2.7. *Interdiction de transmission lors de transferts ultérieurs à des destinataires de données tels que l'UST (articles 21 de la LVP et 25 et 26 de la Directive 95/46/CE)* ... 26